We claim:

1. A validation protocol for determining whether an untrusted authentication chip is valid, or not, including the steps of:

generating a random number in a trusted authentication chip;

applying a keyed one way function to the random number using a key to produce an outcome, in both the trusted authentication chip and an untrusted authentication chip;

comparing the outcomes produced in both the trusted and untrusted chips, and in the event of a match considering the untrusted chip to be valid;

otherwise considering the untrusted chip to be invalid.

2. A validation protocol according to claim 1, where the key is kept secret.

3. A validation protocol according to claim 1, where the domain of the random numbers generated is non-deterministic.

4. A validation protocol according to claim 1, where the keyed one-way function is a symmetric cryptograph, a random number sequence, or a message authentication code.

5. A validation protocol according to claim 1, where the key has a minimum size of 128 bits where the one-way function is a symmetric cryptographic function.

6. A validation system for performing the method according to claim 1, where the system includes a trusted authentication chip and an untrusted authentication chip; the trusted authentication chip includes a random number generator a keyed one-way function and a key for the function; the untrusted authenitcation chip includes the keyed one way function and the key; and a comparison means compares the outcomes produced in both the trusted and untrusted chips, and in the event of a match the untrusted chip is considered to be valid.

7. A validation system according to claim 6, where the key is kept secret.

8. A validation system according to claim 6, where the trusted authentication chip contains a random function to produce random numbers from a seed, and the function advances after every random number is produced so that the next random number will be produced from a new seed.

9. A validation system according to claim 7, where each trusted authentication chip contains a random function to produce random numbers from a seed, and for a group of authentication chips, each chip has a different initial seed, so that the first call to each chip requesting a random number will produce different results for each chip in the group.

10. A validation system according to claim 8, where the domain of the random numbers generated is non-deterministic.

11. A validation system according to claim 6, where the keyed one-way functions is a symmetric cryptograph, a random number sequence, or a message authentication code.

12. A validation system according to claim 6, where the key for the keyed one-way function has at least 128 bits where the one-way function is a symmetric cryptographic function.